

Parallel DIQKD from parallel repetition

Thomas Vidick*

Abstract

We give an arguably simpler and more direct proof of a recent result by Miller, Jain and Shi, who proved device-independent security of a protocol for quantum key distribution in which the devices can be used in parallel. Our proof combines existing results on immunization (Kempe et al., SICOMP 2011) and parallel repetition (Bavarian et al., STOC 2017) of entangled games.

In a recent preprint [JMS17], Miller et al. give a protocol for device-independent quantum key distribution (DIQKD) in which the users provide inputs to, and collect outputs from, their respective devices *in parallel*: Alice (resp. Bob) selects a random string of N inputs $x = x_1, \dots, x_N \in \mathcal{X}$ (resp. $y = y_1, \dots, y_N \in \mathcal{Y}$); each user provides its N inputs to its respective device and collects N outputs $a = a_1, \dots, a_N \in \mathcal{A}$ (resp. $b = b_1, \dots, b_N \in \mathcal{B}$). Once this phase has completed the devices are no longer needed. The protocol concludes by classical phases of parameter estimation, error correction and privacy amplification.

The proof in [JMS17] introduces a number of novel techniques in order to analyze the entropy generation, as well as the robustness, of the protocol, which is based on the Mermin-Peres Magic Square game [Ara02] as a certificate of entropy generation. The goal of this note is to sketch a different proof of the same result, obtained by an elementary combination of existing results. The first result is the technique of “immunization” introduced in [KKM⁺11]: this technique provides a generic method to show that a three-player guessing game based on (e.g.) the Magic Square game cannot be won with probability 1, even by players sharing entanglement; see Lemma 2. The second result is a threshold theorem for the parallel repetition of multiplayer entangled games that satisfy a property called “anchored”; see Lemma 4. Combining these two results gives a proof of security of a similar (though subtly different) protocol for parallel DIQKD than the one in [BVY15]; see Section 3.

In this note we sketch the simple argument, hoping to provide an alternative viewpoint on [JMS17]. We omit the more standard details, and do not comment on the usefulness or practicality of parallel DIQKD.

1 Notation

For a string $x \in \mathcal{X}^n$ and $S \subseteq \{1, \dots, n\}$ we let x_S be the bits of x indexed by S . Given a multi-player game G , we let $\omega_c(G)$ and $\omega^*(G)$ be its classical and entangled value respectively.

We use MS to denote the Magic Square game, which is such that $\omega_c(\text{MS}) = 1$ and $\omega^*(\text{MS}) = 1$. The Magic Square game is a free game (i.e. the input distribution has a product form) in which each player has three possible inputs $x \in \mathcal{X}$ (a row), $y \in \mathcal{Y}$ (a column) and four possible outputs $a \in \mathcal{A}$, $b \in \mathcal{B}$ (an even or odd assignment to the entries in the row or column). It has the useful property that for every $(x, y) \in \mathcal{X} \times \mathcal{Y}$ there exists functions

$$f_{xy} : \mathcal{A} \rightarrow \{0, 1\}, \quad g_{xy} : \mathcal{B} \rightarrow \{0, 1\} \quad (1)$$

*Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA. email: vidick@cms.caltech.edu. Research funded by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, and the IQIM, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

such that for any valid output-input tuple $(a, b|x, y)$ in the game, $f_{xy}(a) = g_{xy}(b)$. In other words, there is always one bit that is expected to match in each players' answers.

2 Guessing games

Definition 1. Let G be a two-player free game, and $0 < \eta \leq 1$. We define the η -guessing game associated with G , G_η , as follows:

1. Alice and Bob receive independent inputs x, y respectively, distributed as in G .
2. With probability $(1 - \eta)$ Eve receives input (x, y) . With probability η she receives no input.
3. The players produce outputs a, b and e respectively.
4. The verifier accepts if and only if $(a, b|x, y)$ is a valid output-input tuple in G , and either $e = a$ or Eve had no input.

The following lemma follows from the “immunization” technique introduced in [KKM⁺11] (see e.g. Lemma 17 in the paper).

Lemma 2. *Let G be a two-player game such that $\omega^*(G) = 1 > \omega_c(G)$. Then for any $0 < \eta \leq 1$ there is a $C_G(\eta) > 0$ (depending on η and the number of questions in G) such that*

$$\omega_c(G) \leq \omega^*(G_\eta) \leq 1 - C_G(\eta).$$

Although our results apply more generally, to fix ideas we focus on a game G instantiated as the Magic Square game MS, and $\eta = 1/8$ (this is an arbitrary choice). Furthermore, in Definition 1 we relax the requirement on Eve to only guess the bit $f_{xy}(a) = g_{xy}(b)$ in common in the players' answers (when they satisfy the winning condition for MS). It can be shown using the same immunization technique that Lemma 2 still holds with this requirement (see also Proposition 4.1 in [JMS17]). Let $C_{\text{MS}}^* = C_{\text{MS}}(1/8) > 0$ be the constant associated to this choice of game and η by Lemma 2, i.e.

$$C_{\text{MS}}^* = 1 - \omega^*(\text{MS}_{1/8}). \quad (2)$$

We now consider the problem of parallel repetition of a multiplayer game.

Definition 3. Let G be a multiplayer game, $n \geq 1$ an integer and $\omega^*(G) \leq t \leq 1$ a threshold value. We define $\tau_{n,t}^*(G)$ to be the entangled value of the following game $G^{(n,t)}$:

- The referee selects n independent tuples of inputs for the players in G , and simultaneously sends each player its n respective inputs; each player replies with n outputs.
- The referee accepts if and only if the fraction of rounds in which the winning condition for G is satisfied by the players' inputs and outputs for that round is at least t .

The following follows from [BVY15, Theorem 23]. The only condition to verify is that for any two-player free game G and $\eta > 0$ the game G_η is an anchored game, which is immediate from the definition (this is the sole reason for introducing G_η from G).

Lemma 4. *Let G be a two-player free game, $0 < \eta \leq 1$ and $\delta > 0$ such that $t = \omega^*(G_\eta) + \delta \leq 1$. Then*

$$\tau_{n,t}^*(G) \leq e^{-\Omega(\delta^9 n)},$$

where the implicit constant in the exponent depends on η and $|G|$ but not on n .

3 Parallelizing DIQKD

We consider a simple protocol for parallel DIQKD, Protocol 1, directly inspired from the protocol Magic-QKD in [JMS17]. The following theorem states a bound on the quantum conditional min-entropy of Alice's outputs at the end of the protocol. Applying standard steps of error correction and privacy amplification it is straightforward to obtain a positive key rate from the theorem. (Using that the Magic Square game has the property that in a winning strategy one of Alice's output bits is required to equal one of Bob's output bits, the additional loss due to error correction will scale as $O(\epsilon n)$.)

Theorem 5. *Let MS be the two-player Magic Square game, $C_{\text{MS}}^* > 0$ the constant defined in (2), and $\gamma, \epsilon > 0$ such that $\epsilon < C_{\text{MS}}^*/2$. Suppose that Protocol 1 (with parameter $\eta = 1/8$) is executed with arbitrary devices such that the probability of Alice and Bob aborting in Step 5 is at most p_a .*

Let $\rho_{K_A E}$ be the joint state of Alice's raw key and Eve's side information at the end of the protocol, conditioned on Alice and Bob not aborting in Step 5. Then

$$H_{\infty}^{\epsilon_s}(K_A|E)_{\rho} \geq \Omega((C_{\text{MS}}^* - 2\epsilon)^9 n) - \log p_a^{-1} - O(\gamma n),$$

where $\epsilon_s = p_a^{-1} \exp(-\Omega(\epsilon^2 \gamma n))$. Moreover, honest players using $(\epsilon/2)$ -noisy devices are accepted in the protocol with probability $1 - \exp(-\Omega(\epsilon^2 \gamma n))$.

The bound claimed in the theorem is analogous to [JMS17, Theorem 1.2]. We do not work out explicit constants, but due to the protocol being simpler, and the analysis more direct, we expect that they could be made to improve upon [JMS17].

Proof. Let $G = \text{MS}$ and $\eta = 1/8$. Observe that right after Step 2 in Protocol 1 the inputs in the possession of Alice, Bob and Eve are distributed exactly as in the n -fold parallel repetition of the game G_{η} : Alice and Bob have n independent inputs to G , while Eve has both player's inputs in a subset S of the rounds of expected size $(1 - \eta)n$, and no input for the remaining rounds. Let $t = 1 - 2\epsilon$. The winning condition for $G_{\eta}^{(n,t)}$ (Definition 3) is implied by the conjunction of the following two conditions:

- Alice and Bob's outputs satisfy the winning condition for G in a fraction at least t of the rounds;
- Eve's output e_i matches $f_{x_i y_i}(a_i)$ in all rounds $i \in S$.

We evaluate the probability that the first condition is not satisfied, yet the players do not abort at Step 5. For $i \in \{1, \dots, n\}$ let W_i be the indicator random variable for the event that inputs and outputs for Alice and Bob in the i -th round satisfy the winning condition for G . Since the rounds T in which the players evaluate the game condition are chosen uniformly, it follows from a standard concentration bound (see e.g. [TL15, Lemma 7]; note that no independence is required of the W_i) that

$$\Pr \left(\sum_{i \in T} W_i > (1 - \epsilon)|T| \wedge \sum_{i \in \{1, \dots, n\}} W_i \leq (1 - 2\epsilon)n \right) = e^{-\Omega(\epsilon^2 \gamma n)}, \quad (3)$$

where we may assume that the bound on the right-hand side incorporates the probability that Alice and Bob abort due to $|T| < \gamma n$, which given $\eta = 1/8$ and $\gamma \leq 1/2$ is exponentially small in n . Let $\tilde{\rho}_{K_A E}$ be the joint state of Alice's raw key and Eve's side information at the last step of the protocol, conditioned on the event that the players do not abort in Step 5, and the condition $\sum_{i \in \{1, \dots, n\}} W_i > (1 - 2\epsilon)n$ holds. Let \tilde{p}_a be the probability of the latter conjunction of events. By definition of the winning condition for $G_{\eta}^{(n,t)}$ and the relation between guessing entropy and conditional min-entropy [KRS09] it follows that

$$H_{\infty}(K_A|E)_{\tilde{\rho}} \geq -\log(\tau_{n,t}^*(G)/\tilde{p}_a).$$

Protocol 1 Parallel DIQKD protocol

Arguments: D – untrusted device $n \in \mathbb{N}_+$ – number of rounds $\eta \in [0, 1]$ – fraction of rounds in which Alice and Bob’s inputs are not leaked to Eve (*game* rounds). $\gamma \in (0, 1/2]$ – fraction of rounds in which Alice and Bob test the game condition (*test* rounds). $\varepsilon \in [0, 1/2]$ – noise tolerance for honest devices.

- 1: For every $i \in \{1, \dots, n\}$, Alice and Bob independently select inputs x_i and y_i in the game G .
 - 2: Alice selects a random subset $S \subseteq \{1, \dots, n\}$ by choosing each round independently with probability $(1 - \eta)$. She sends (S, x_S) to Bob. Bob replies with y_S .
 - 3: Alice and Bob provide their respective strings of inputs, x and y , to their device.
 - 4: Alice and Bob collect output strings a and b from their respective device.
 - 5: Alice selects a random subset $T \subseteq S$ of size $|T| = \gamma n$ (if $|S| \leq \gamma n$ they abort). She sends (T, a_T) to Bob. Bob replies with b_T . They abort the protocol if fewer than $(1 - \varepsilon)|T|$ of the rounds in T satisfy the winning condition for G .
 - 6: Alice (resp. Bob) sets $(K_A)_i = f_{x_i y_i}(a_i)$ (resp. $(K_B)_i = g_{x_i y_i}(a_i)$), for $i \in S$, where f, g are as in (1). The resulting S -bit strings form their raw key.
-

Applying Lemma 4, $\tau_{n,t}^*(G) = \exp(-\Omega((t - (1 - C_{\text{MS}}^*))^9 n))$. Since by (3) we have $\|\tilde{\rho} - \rho\|_1 = p_a^{-1} \exp(-\Omega(\varepsilon^2 \gamma n))$ (with $\rho = \rho_{K_{AE}}$ as defined in the theorem), we deduce the bound claimed in the theorem, where the subtraction of an $O(\gamma n)$ term accounts for outputs leaked to Eve in Step 5.

Finally, the “moreover” part of the theorem follows from a standard concentration argument. \square

References

- [Ara02] P. K. Aravind. The magic squares and Bell’s theorem. Technical report, arXiv:quant-ph/0206070, 2002.
- [BVY15] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Anchoring games for parallel repetition. *To appear in STOC’17*, 2015.
- [JMS17] Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel device-independent quantum key distribution. *arXiv preprint arXiv:1703.05426*, 2017.
- [KKM⁺11] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM J. Comput.*, 40(3):848–877, 2011.
- [KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347, 2009.
- [TL15] Marco Tomamichel and Anthony Leverrier. A rigorous and complete proof of finite key security of quantum key distribution. *arXiv preprint arXiv:1506.08458*, 2015.